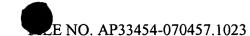


WE CLAIM:

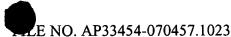
- 1. A method of conducting an electronic transaction over a public communications network, with a payment account number having a certain amount of available funds, using a payment network linked to a check site, comprising:
 - (a) generating a secret key associated with said payment account number;
- (b) using said secret key to generate a message authentication code specific to said transaction;
- (c) generating an authorization request message including said message authentication code;
- (d) forwarding said authorization request message over said payment network to said check site for verifying the authenticity of said message authentication code;
- (e) verifying the message authentication code by said check site using said secret key;
- (f) responding to said authorization request message over said payment network based on said available funds and said transaction amount.
- 2. The method of claim 1, wherein said authorization request message is routed over said payment network based on a special bank identification number corresponding to said check site.

NY02:332016.1 32



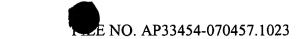
- 3. The method of claim 2, further comprising: providing software at a user location for generating said secret key.
- 4. The method of claim 3, wherein said payment account number is issued by an issuer and said response is provided by said issuer.
- 5. The method of claim 4, wherein said authorization request message includes an expiration date field and said message authentication code is placed in said expiration date field.
- 6. A method of conducting an electronic transaction over a public communications network with a check site and a payment account number having a BIN associated with said check site comprising:
 - generating a per-card key associated with said payment account number; (a)
 - generating a message authentication code (MAC) using said per-card key; (b)
- generating a MAC verification request including said payment account (c) number and said MAC;
 - verifying said MAC; (d)
- based on said verification, creating an expected transaction sequence (e) number (ETSN) for said MAC;
 - (f) providing said check site with reference data associated with said ETSN;

33 NY02:332016.1



- generating a second message authentication code using said ETSN and (g) said per-card key;
- (h) routing said second message authentication code to said check site based on said BIN associated with said check site;
- (i) determining said per-card key associated with the payment account number of an unverified message authentication code having associated ETSN and reference data;
- verifying said second message authentication code by said check site using (i) said determined per-card key, and said associated ETSN and reference data.
- 7. The method of claim 6 further including, after the step of generating a second message authentication code, the following steps:
- converting said second message authentication code into a pseudo (a) expiration date using said reference data;
- generating an authorization request having an expiration date field (b) containing said pseudo expiration date; and
- responding to said authorization request and verifying said second (c) message authentication code based on said pseudo expiration date.
- 8. The method of claim 7 wherein the step of generating a message authentication code further includes using an expiration date, application version number and transaction sequence number associated with said payment account number.

34 NY02:332016.1



- 9. The method of claim 8 wherein said MAC verification request further includes said application version number and said expiration date.
- 10. The method of claim 9, wherein said step of verifying said MAC includes using said per-card key.
- 11. The method of claim 6, wherein said reference data includes a reference data and a number of months indicator.

NY02:332016.1 35